REMARKS

The Office Action dated January 12, 2004 has been received and carefully noted. The following remarks, are submitted as a full and complete response thereto. No new matter has been added, and no new issues are raised which require further consideration and/or search. Claims 19 and 20 have been allowed. Claims 1-18 are submitted for consideration.

Applicants wish to thank the Examiner for allowing claims 19 and 20.

Applicants wish to thank the Examiner for indicating that claims 7, 9, 11 and 14-16 would be allowable if rewritten in independent form. Since the rejection of claim 1, upon which claims 7, 9, 11 and 14-16 depend, is traversed as outlined below, Applicants respectfully request that the objection of claims 7, 9, 11 and 14-16 be withdrawn and that claims 1-18 be allowed.

Claims 1-6, 8, 10 12-13 and 17-18 were rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,169,735 to Allen, Jr. et al. in view of U.S. Patent No. 6,438,612 to Ylonen et al. The rejection is traversed as being based on references that neither teach nor suggest the novel combination of features clearly recited in independent claims 1, 17 and 18. Claim 1, upon which claims 2-16 depend, recites a method including the step of configuring a circuit emulation service (CES) over an internet protocol (IP) network based on properties of the IP network. The CES is configured to establish a tunnel between a local interworking function and a remote interworking function. The method also includes the steps of encapsulating data received at a constant

bit rate at the local interworking function into a plurality of IP packets configured according to the CES, wherein the plurality of IP packets includes a first IP packet having a variable length and transporting the IP packets from the local interworking function to the remote interworking function according to the CES.

Claim 17 recites an article of manufacture comprising a machine readable storage medium having stored thereon a plurality machine executable instructions. The instructions, when executed, implement a method including the step of configuring a circuit emulation service (CES) over an internet protocol (IP) network based on properties of the IP network. The CES is configured to establish a tunnel between a local interworking function and a remote interworking function. The method also includes the step of encapsulating data received at a constant bit rate at the local interworking function into a plurality of IP packets configured according to the CES, wherein the plurality of IP packets includes a first IP packet having a variable length. The method further includes the step of transporting the IP packets from the local interworking function to the remote interworking function according to the CES.

Claim 18 recites an apparatus including a first circuitry to configure a circuit emulation service (CES) over an internet protocol (IP) network based on properties of the IP network. The CES is configured to establish a tunnel between a local interworking function and a remote interworking function. The apparatus also includes a second circuitry to encapsulate data received at a constant bit rate at the local interworking function into a plurality of IP packets configured according to the CES, wherein the

plurality of IP packets includes a first IP packet having a variable length. The apparatus further includes a third circuitry to transport the IP packets from the local interworking function to the remote interworking function according to the CES.

As will be discussed below, the cited prior art references of Allen, Jr. et al. and Ylonen et al. fail to disclose or suggest the elements of any of the presently pending claims.

Allen, Jr. et al. teaches an ATM-based distributed virtual tandem switching system which includes an originating end office, a terminating end office, an ATM switching network, a trunk interworking function device, a centralized control and signaling interworking function device. Col. 6, lines 3 - 8 and Col. 7, line 45 – Col. 8, lines 14. The trunk interworking function device receives end office voice trunks from TDM channels and converts the trunks to ATM cells. Col. 6, lines 8-11 and Col. 7, line 67 - Col. 8, line 1. The centralized control and signaling interworking function device functions as an interface between narrowband and broadband signaling for call processing and control within the ATM switching network. Col. 6, lines 11 – 15 and Col. 8, lines 10 - 22. The trunk interworking function device includes circuit emulation services to emulate the circuit characteristics in order to carry constant bit rates traffic such as voice, an ATM adaptation layer 1 (AAL1) and alternatively, an ATM adaptation layer 2 (AAL2). Col. 6, lines 17 – 22 and Col. 9, line 15 - Col. 10, line 22. The AAL2 enables voice to be carried as variable bit rate data while maintaining its delay sensitive nature. Col. 10, lines 29 - 66. According to Col. 10, lines 64 - 66 of Allen, Jr. et al.,

"essentially what AAL1 or AAL2 allow is the choice of carrying voice trunks through an ATM network as constant bit rate traffic or variable bit rate traffic." Therefore, if voice is sent as constant bit rate traffic, then CES service using AAL1 is employed and if voice is sent as real time variable bit rate traffic then AAL2 as the ATM adaptation layer is employed. Col. 10, line 66 – Col. 11 line 5.

To transmit voice from an originating end office to a terminating end office, the system transmits voice from an originating location to an original trunk that leaves an end office switch. The voice is transported by employing the circuit emulation service in the trunk interworking function device. The system then converts the originating trunk to ATM cells and interfaces between the narrowband and broadband signaling for call process and control within the ATM network. Thereafter the voice within the ATM cell is transmitted across the ATM network using the broadband signaling and the ATM cells are converted to a destination trunk. Then the voice is transmitted from the destination trunk to the destination or terminating end office. Col. 6, lines 30-50.

Allen, Jr. et al. also teaches that the trunk interworking function device implements a modem pool of Internet Protocol (IP) packets carried with bursty data and converts them to ATM connections. These ATM connections can then be carried by the ATM network to the Internet service providers. The ATM connections may be delivered to the Internet service providers as ATM or converted back to IP packets. Col. 16 line 55 – Col. 17 line 8.

Ylonen et al. teaches that there is a problem with packet labeling in virtual networks because it is difficult to identify the virtual network to which a packet belongs. A typical packet includes a header portion which includes the source and destination addresses, a data portion and possibly a checksum. To temporarily transmit the typical packet over a logical network where the source and destination address are invalid, the packet must be encapsulated and relabeled. The process of encapsulating data packets for transmission over a different logical network is called tunneling and involves adding a new IP header in front of the original packet, setting the protocol field in the new header and sending the packet to the desired destination. When packets are tunneled between routers, the packet is typically wrapped in an outer IP header, wherein the outer IP source address is set to the IP address of the sending node, the outer IP destination address is set to the address of the endpoint of the tunnel and the outer protocol identifier is set to identify the tunneling method. Col. 2, lines 1-52.

Ylonen et al. further teaches that in addition to the problem with packet labeling, there is also a problem with the security of data traffic in public networks. Therefore, IP security protocol (IPSEC) was developed for adding security to IP protocol. IPSEC performs authentication and encryption on packet level by generating a new IP header and adding an Authentication Header (AH), or Encapsulating Security Payload (ESP) header to the front of the packet. The original packet is cryptographically authenticated and optionally encrypted. The method used to authenticate and possible encrypt the packet is identified by a security parameter index value in the AH and ESP headers. The

ESP may appear anywhere in the IP packet after the IP header and before the final transport layer protocol. ESP consists of an unencrypted header followed by encrypted data. The encrypted data includes the protected ESP header field which includes a 32 bit Security Association Identifier and a variable length Opaque Transform Data field and the protected user data. Col. 2, line 60 – Col. 3, line 46.

Applicants submit that the combination of Allen, Jr. et al. and Ylonen et al. does not teach or suggest the combination of features in claims 1, 17 and 18 and the claims dependent thereon. Claims 1, 17 and 18, in part, recite that a CES is configured to establish a tunnel between a local interworking function and a remote interworking function and the step of encapsulating data received at a constant bit rate at the local interworking function into a plurality of IP packets configured according to the CES, wherein the plurality of IP packets includes a first IP packet having a variable length. The Office Action correctly stated that Allen, Jr. does not teach or suggest the CES being configured to establish a tunnel between a local interworking function and a remote interworking function and encapsulating data received at a constant bit rate at the local interworking function into a plurality of IP packets configured according to the CES, wherein the plurality of IP packets includes a first IP packet having a variable length as recited in claims 1, 17 and 18. However, the Office Action states that Ylonen et al teaches that during tunneling the new header added to the front of the original packet include an AH or ESP header in front of the packet, wherein the ESP may appear anywhere in an IP packet after the IP header and whereby the two parts of the ESP header

are the 32-bit SPI and the variable length Opaque Transform Data Field. Upon review of Ylonen et al., col. 2, lines 17-52 of Ylonen teaches that to solve the problem associated with packet labeling in a virtual network, during tunneling a new IP header is added to the front of the original packet. However, according to Ylonen et al., in addition to the problems associated with packet labeling in virtual networks, there is also a problem with the security of data traffic in public networks. Therefore, Ylonen et al. teaches that IPSEC provides for cryptographic authentication and confidentiality of traffic between two communicating nodes. According to Ylonen et al., IPSEC performs authentication and encryption on packet level by generating a new IP header and adding an Authentication Header (AH), or Encapsulating Security Payload (ESP) header to the front of the packet, wherein the ESP may appear anywhere in the IP packet after the IP header and before the final transport layer protocol and the ESP consists of an unencrypted header that includes a 32 bit Security Association Identifier and a variable length Opaque Transform Data field. Ylonen et al. teaches that the "new IP header" generated by the IPSEC is different from the IP header used during tunneling. The "new IP header" of Ylonen et al. with the variable length Opaque Transform Data field is used for authentication and possibly encryption and not for encapsulating data during tunneling in a virtual network as the Office Action suggests. There is simply no teaching or suggestion in Ylonen et al of encapsulating data received at a constant bit rate at the local interworking function into a plurality of IP packets configured according to the CES,

wherein the plurality of IP packets includes a first IP packet having a variable length as recited in claims 1, 17 and 18.

In the Response to Arguments, the Office Action also states that Allen, Jr. et al. does not teach away from variable length packets. However, Allen, Jr. et al., teaches that "essentially what AAL1 or AAL2 allow is the choice of carrying voice trunks through an ATM network as constant bit rate traffic or variable bit rate traffic." Col. 10, lines 64-66. There is simply no teaching or suggestion in Allen Jr. et al. of encapsulating data received at a constant bit rate at the local interworking function into a plurality of IP packets configured according to the CES, wherein the plurality of IP packets includes a first IP packet having a variable length as recited in claims 1, 17 and 18. Therefore, Applicants assert that the rejection under 35 U.S.C. §103(a) should be withdrawn because neither Allen Jr. et al. nor Allen Jr. et al. Ylonen et al., whether taken singly or combined, teaches or suggests each feature of claims 1, 17, and 18 and hence, dependent claim 2-16 thereon.

As noted previously, claims 1-18 recite subject matter which is neither disclosed nor suggested in the prior art references cited in the Office Action. It is therefore respectfully requested that all of claims 1-18 be allowed and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by

telephone, the applicants undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Arlene P. Neal
Registration No. 43,828

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

APN:lls

Enclosures: Revocation and New Power of Attorney